Hash functions: $h: \{0,1\}^* \to \{0,1\}^b$

We want **collision resistance**: $h(x) = h(x')$ for $x \neq x'$ is hard

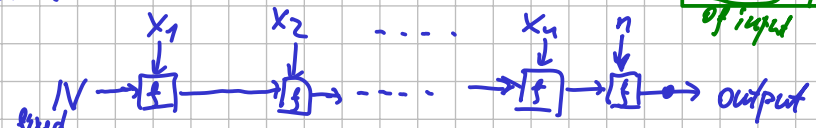
$f(a,b) = f(a',b')$

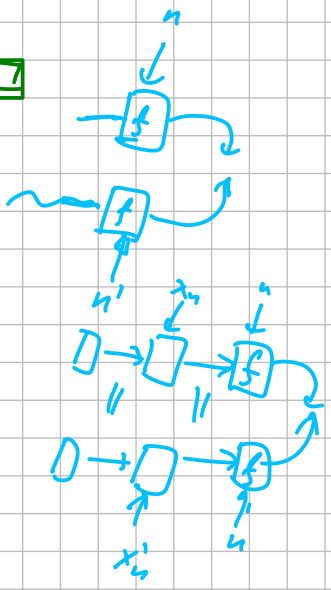
Merkle-Damgård construction

Given a **compression function** $f: \{0,1\}^b \times \{0,1\}^b \to \{0,1\}^b$

Construct h:

typical input: [rest of input | padding | n]





Thm: If f is collision-resistant, then h is c.r.

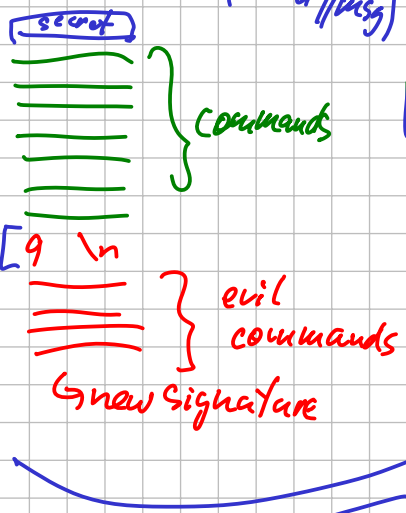
Pf: If we have $h(x_1 \| \dots \| x_n) = h(x'_1 \| \dots \| x'_{n'})$ (different)

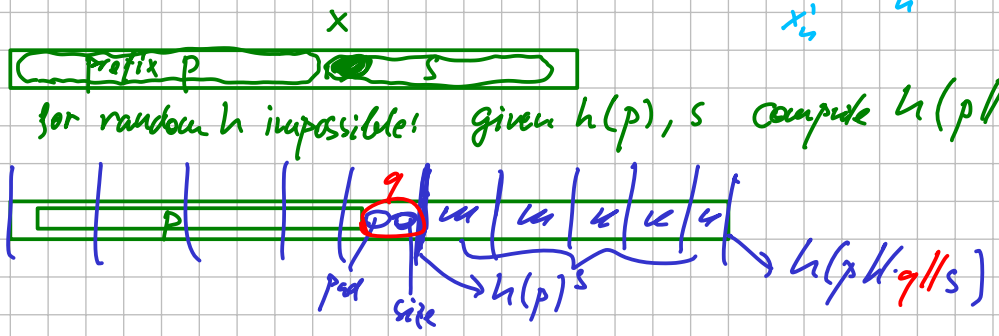
Then either $n \neq n'$: collision in f $f(-,n) = f(-,n')$

or $n = n'$: — " — .

Length extension property:

sign = h(secret ‖ msg)





How to obtain compression function f?

Davies-Meyer construction from a block cipher

$f(u,v) := E_u(v) \oplus v$

Thm: With an ideal block cipher, (a random permutation for every key)

f is collision-resistant.

In particular: for an attack evaluating E/D q times: $q \leq 2^{b/2}$

$\Pr[\text{collision found}] \leq q^2/2^b$

① why $\oplus v$?

$f'(u,v) := E_u(v)$

$E_u(v) = y$

$D_u(y) = v'$

then $f'(u,v) = f'(u',v')$ (both $= y$)

② with DES

$E_{\bar{k}}(\bar{x}) = \overline{E_k(x)}$

$f(\bar{a},\bar{b}) = E_{\bar{a}}(\bar{b}) \oplus \bar{b}$

$= \overline{E_a(b)} \oplus \bar{b}$

$= E_a(b) \oplus b = f(a,b)$

$\bar{x} = x \oplus 1\dots1$

$\bar{x} \oplus \bar{y} = x \oplus 1\dots1 \oplus y \oplus 1\dots1$

$= x \oplus y \oplus 0\dots0$

$= x \oplus y$

③ for $v := D_u(0)$ $f(u,v) = E_u(v) \oplus v = 0 \oplus v = v$

Proof:

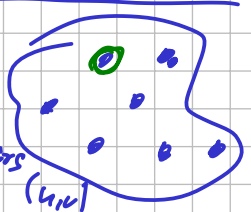
wLOG we ask no redundant questions

If we ask $E_u(v) \to f(u,v) = E_u(v) \oplus v$

if $D_u(v) \to f(u, D_u(v)) = v \oplus D_u(v)$

We find a first collision in step i $(1 \leq i \leq q)$

we found $f(u_i, v_i)$ matching a known value (one of $i-1$ of them)



for every pair (old ans, new ans)

for a fixed known value:

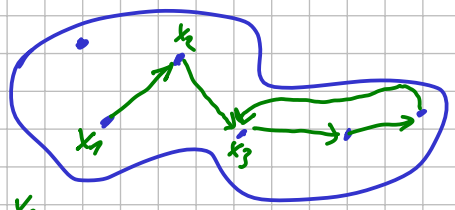
$\Pr[\text{collision}] = \frac{1}{\#\text{of possible answers}} \leq \frac{1}{2^b - i - 1} \leq \frac{1}{2^{b-1}}$ $\quad i \leq 2^{b/2} \leq 2^{b-1}$

$\Pr[\text{collision}] \leq \frac{1}{2^{b-1}} \cdot \#\text{pairs} \leq \frac{q^2}{2 \cdot 2^{b-1}} = q^2/2^b$ $\quad \binom{q}{2} \leq q^2/2$

Finding collision

① brute force $h(x_1), h(x_2), \dots$ & look for match → by Birthday paradox, expect a match in $\sim 2^{b/2}$ steps.
with lots of memory

② with constant memory:



$G=(V,E)$ — possible blocks — $(x, h(x))$

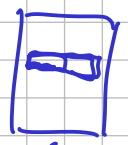
$\deg^{out}(x) = 1$

lollipop graph

- tortoise: 1 step at a time
- hare: 2 steps at a time

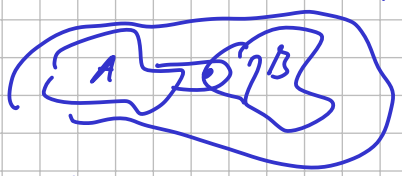
& wait until they meet for the 1st time
after t steps, both are on the cycle
then they must meet

③ meaningful messages → parametrized message



$(x, h(\text{parametrize}(x)))$

④ $h(\text{evil}) = h(\text{innocent})$



If A, B random subsets of X ($|X| = n$).
$|A|, |B| \sim \sqrt{n}$
⇒ likely $|A \cap B| \geq 1$

→ $\sim 2^{b/2}$ innocent msgs —hash→ A
$\sim 2^{b/2}$ evil msgs —hash→ B

⑤ If h is M.-D., we can produce lots of collisions ~ as easy as 1 coll.

in $\sim 2^{b/2}$ steps: $x_1 \neq x_1'$ $f(IV, x_1) = f(IV, x_1') = y_1$
— " — : $x_2 \neq x_2'$ $f(y_1, x_2) = f(y_1, x_2') = y_2$

k times → $x_1 \; x_1'$; $x_k \; x_k'$

2^k combinations which hash to the same result

in time $\sim k \cdot 2^{b/2}$ we produced 2^k-fold collision

Concatenation of 2 hashes h_1, h_2 with b-bit output.
$h(x) := h_1(x) \,||\, h_2(x)$ How strong is this? 2b bits?
NOT if either h_1 or h_2 is M.-D.!

Suppose h_1 is M.D.
By ⑤ with $k = b/2$ we can find $2^{b/2}$ colliding msgs for h_1 in time $b/2 \cdot 2^{b/2}$
↳ then h_2 will likely collide for 2 of these.
↳ collision in h in time $b/2 \cdot 2^{b/2}$

Real-world hashes

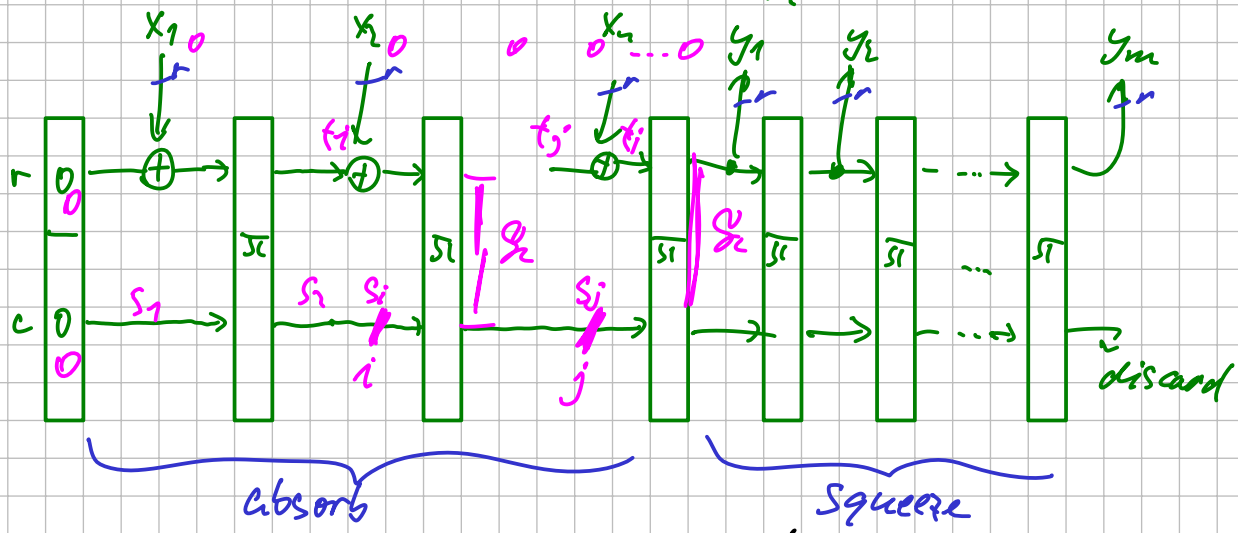
MD5 (Rivest 1992) 128b of result (small!) BROKEN 2004 → can find collision (but not invert)
↳ Message Digest
SHA-1 (NSA) 160b of result BROKEN 2017
SHA-2 (NSA) 224 ... 512b of result not broken (yet)
Competition by NIST → SHA-3 published 2015

Sponge construction

- permutation π on blocks of size $w = r + c$

phase 1: absorbing the input
phase 2: squeezing out the output

width w, rate r, capacity c



Next week: SHA-3 MACs (symmetric signatures)

Security against 2^{nd} pre attacks: ① in $2^{r/2}$ steps: attack output
② internal collisions by Birthday pdx. in $2^{c/2}$ blocks find $i < j$: $s_i = s_j$

first: 0^i
2nd: $0^{j-1}(t_i \oplus y_j)$

} output of π is the same ⇒ squeeze out the same output

Known: for π random
sec. level of sponge $\geq \min(r/2, c/2)$.